# Identity Theft on the Internet

*Md. Ashik Mahmud, Sanjida Junak Priya , Kazi Shifatur Rahman, Hasan Mahmud Bhuiya*

KEYWORDS

Cyber Security

Cyber Crime

Identity Theft

Internet fraud

Computer forensics

Malware

Reverse Engineering

Traffic analysis

Network monitoring

ABSTRACT

This paper explores and investigates identity theft through a compilation of statistical data and previousstudies conducted regarding typical methodologies used, the effects of identity theft, and to develop ideal program components to provide services for the prevention, investigation, and resolution of identity theftincidents. The problem at hand is the increased number of vulnerabilities and security hazards for individuals engaging in e-commerce, business transactions over the World Wide Web. Since the majorityof people aren't paying their bills by mailing in their payment to the vendor, they pay for the items theypurchase online, which makes them open to hackers and social engineering attacks. They place their credit card/debit card numbers, their phone number and home address, and even their birth date information on company websites. All these security vulnerabilities make the risk of identity theft increasingly high. Identity theft is when an individual's personal(confidential) information, such as socialsecurity or account numbers, is stolen and used against them. The research examines both mundane methods involved in the commission of identity theft as well as the use of cyber technology as the methodsof operation. This research paper examines instances of known losses and harm suffered by individuals, businesses, and our society, as well as how law enforcement is challenged by this type of fraud within the United States. Based on previous studies conducted as well as both qualitative and quantitative data available from law enforcement and regulators specializing in such investigations, the author explains the need for aggressive enforcement concerning identity theft and provides recommendations forcomponents for a program to support such efforts. The author suggests possible future research improvements by addressing the need to obtain more specific and accurate data concerning identity theftincidents by jurisdiction as well as investigation, arrest, and prosecution outcomes. The author contendsthat improved data regarding types of identity theft may be obtained via additional and more recent cybercrime schemes and incidents of identity theft.

## 1.Introduction

The issue at stake is the rise in security risks and vulnerabilities for those conducting e-commerce, or business transactions over the World Wide Web. The majority of consumers pay for their purchases online rather than by mailing checks to the vendor, leaving them vulnerable to social engineering and hacker attacks. On company websites, they publish information such as their birth date, phone number, home address, and credit card or debit card numbers. The risk of identity theft is rising due to all these security flaws. Identity theft occurs when someone's private (confidential) data, like their social security number or bank account number, is taken and used against them.

Any internet user's identity can be taken in a matter of seconds without their knowledge. If a user is connected to the internet, there are a number of tools accessible that allow anyone to steal their data. It is not necessary for the attacker to possess in-depth understanding of networking or internet technology. The majority of Internet users have a serious problem with identity theft.

Any internet user's identity can be taken in a matter of seconds without their knowledge. If a person is connected to the internet, there are a number of tools accessible that enable anyone to steal that user's data. It is not necessary for the attacker to possess in-depth understanding of networking or internet technology. The majority of Internet users have a serious problem with identity theft. This essay aims to educate readers on the risks of having your identity stolen online. This effort aims to increase awareness of and understanding of identity thefts and related fraud around the globe. According to the U.S. Division of Justice, "Identity fraud and character extortion are terms used to suggest a wide range of wrongdoing in which someone improperly obtains and utilizes someone else's close to home information here and there that includes misrepresentation or trickiness, typically for financial increase. Character thieves steal the client's sensitive information and carry out various acts in the client's best interests without the client's knowledge.

Identity theft is having a rising effect on the developing e-commerce sectors and procedures. Online purchases are being made by more people on mobile devices that have access to the Internet. Personal and confidential information becomes subject to hostile hacker assaults when it is posted on vendor websites. Hackers and crackers obtain users' private information in a variety of methods. Social engineering, phishing, and pharming are a few techniques for information collecting. Whose responsibility is it to keep the data safe from theft? To prevent malware infection, many people install firewall software on their personal computers. Larger businesses and institutions, including banks, owe it to their customers to see to it that countermeasures are taken to cut down on fraud and identity theft. It is the obligation of both consumers and businesses to make sure they are doing everything they can to ensure the security of commercial transactions. What steps can be made to stop identity theft before it becomes so widespread? Because of the rise in attacks, the possibility of identity theft, and virus attacks, security is becoming increasingly important in all facets of Internet privacy and online transactions. Checking that any website dealing with the entry of sensitive information has a web address that starts with "https" rather than merely "http" is one of the steps a person may take to ensure security. Governmental organizations continuously keep an eye on fraud and aspects of fraud connected to computer crime and identity theft. By creating a new variation known as "cyberspace identity theft," the development of the Internet has significantly altered the trend. People who use the Internet enter a digital, networked work environment known as "cyberspace." Users "browse" the internet to trade information, engage, amuse themselves, purchase and sell goods and services, access and use public and private transportation, share interests, and conduct financial transactions in a variety of domestic and foreign businesses. This private information is utilized fraudulently for a variety of purposes, including creating new accounts, controlling the victim's credit accounts, obtaining government benefits, and overturning the law by using a fictitious identity. Unfortunately, identity fraud techniques are hidden from the victim, and people usually become aware of them when they reject new credit cards or loans, lose their jobs, or receive debt collection requests for debts that they haven't created. Each year, victims spend billions of dollars in damages to make up for the effects of identity theft and the abuse of personal information. Private information is significant and essential to many firms' relationships. These partnerships can benefit from the advancement of information technology, but regrettably, cybercrime is also on the rise. Because the information system plays a crucial role in the organization's fundamental function and because computers play a larger role in our daily lives, it is crucial to emphasize how critical it is to secure the information system. Online identity theft is a global cybercrime that is rapidly expanding. Both the organization and the individual are responsible for taking the necessary precautions to protect their privacy and for taking action to prevent any data breaches. Credit card fraud will account for 41.8% of all occurrences of online identity theft in 2020, making it by far the most prevalent sort of theft.

## 2. Literature Review

The terms "identity theft" and "identity fraud" are distinct from one another legally, they have come to be used interchangeably in everyday speech. 1 Some people think of identity theft as a subset of identity fraud. Legal codes typically distinguish between theft and fraud by characterizing the latter as taking from the victim through deception or cunning, such as when one borrows money from the victim with no intention of returning it. Contrarily, simple theft refers to the unintentional stealing of anything directly from the victim. It seems clear that both of these takings are covered by federal law. Identity theft is frequently the result of the commission of several different crimes, many of which, if not all, are crimes that we are all familiar with. The crimes that are frequently linked to identity theft include check and card fraud, financial crimes of various kinds, telemarketing and Internet scams, theft of vehicles and auto parts made possible by false documentation, thefts or robberies of various kinds where identification information is either accidentally or purposefully stolen, counterfeiting and forgery, and human trafficking (Newman and Clarke, 2003).

It is obvious that the crimes associated with identity theft are not at all new, but rather, ancient crimes that have been made worse by the use of, or theft of, stolen identities. However, in our opinion, the federal statute was more likely inspired by the widespread media coverage of identity theft victims in the late 1990s than by those earlier offenses. These victims were frequently victimized over a period of months or even years, and they were either unable to recover their identities or were unable to persuade the authorities in charge of credit issuing and reporting of their loss. The Identity Theft Act of 1998 was eventually passed as a result of Congressional hearings that were sparked by the publicity.

These hearings produced three important facts. First, local law enforcement has been sluggish to identify people as victims because the card issuer, rather than the cardholder, was typically the one who suffered the most of the actual financial loss, such as from credit card fraud. Instead of people, businesses were seen as the victims. Second, testimony from people at the hearings showed that their identities were exploited for a long time until they lost their usefulness. They had indeed been victimized repeatedly. Third, it was not unusual for victims to become aware of their mistreatment years after the crime, which made it more challenging to conduct an investigation. [2]

The literature on identity theft and the associated field of computer privacy is broad and spans a wide range of academic fields and information sources. These include topics including legislation, governmental policy, the online and computer world, as well as the recently-emerging fields of studying security and online commerce. Due to the rise in online fraud and security breaches, the latter topic of study has recently attracted a lot of attention in the literature. However, despite the recent upsurge in studies, publications, and theses on identity theft and computers, many pundits point out that there is still no conclusive or well-established body of knowledge or documentation on identity theft. How Well Do Consumers Protect Themselves from Identity Theft? by George R. Milne, a Journal of Consumer Affairs article, makes this crucial point (2003) The current state of this field's study is succinctly described by Milne.

The aforementioned essay also provides a great outline of the main concerns and difficulties encountered in the identity theft research. Additionally, there has been a resurgence in publications and studies on this topic, which are now more relevant given the development of e-commerce and personal online usage. In this regard, there has been an increase in the number of thorough and reliable internet sites and database sources that deal with the battle against this sort of crime and give a huge array of documents, as well as an increasing number of references and up-to-date information. A broad and helpful summary of the identity theft issue is provided by a number of studies, papers, and surveys. One article that gives a thorough review of the issue is Internet Commerce Grows 88 Percent by

Dollar Volume and 39 Percent by Transaction Volume: Fraud Remains a Concern. The article focuses on a key component of how security issues like ID theft are seen and understood by the general public in addition to discussing the amount of identity theft. Identity theft awareness and understanding are two of the most crucial elements in dealing with and preventing this pernicious crime, as will be covered in the various sections of this study. The aforementioned article offers some relevant and very recent information on the prevalence of ID theft.

The United States, for instance, "remained the top source country for security events generated with an overwhelming 79 percent, followed by Canada (5.7 percent), Taiwan (2.6 percent), Korea (2.5 percent), and the U.K. (2.4 percent), the author writes. (Internet Commerce Grows 39% in Transaction Volume and 88% in Dollar Volume: Fraud Remains a Concern) FraudWatch International is another website that offers a variety of current and pertinent information on these topics. [1] One of the finest online resources, this site's Identity Theft section is regularly updated with the most recent data and information, and it offers a lot of information about ID theft tactics including phishing as well as potential remedies to these issues. Debit's Growing Popularity by Lauren Bielski was a particularly helpful article for determining the effects of identity theft and fraud on the business and financial security (2006). This article examines the significant effects of fraud and identity theft on numerous industries as well as some startling data.

“Looked at as a group these incidents suggest a security flame-out and the perception that electronic information housed in computers is vulnerable. They also suggest that fraud seems to be mutating at a rat [2].

How Effectively Do Consumers Defend Against Identity Theft? In addition to exposing the different consequences of identity theft on consumers, the article [3] also looks in-depth at the steps that can be taken to prevent this intrusive crime. The Economist (2001) says that identity theft, defined as the use of another person's identity to commit fraud or theft, continues to be one of the fastest increasing white-collar crimes in the United States. This study, like many others, reiterates the severity of the issue. [4]

The impact of this is thoroughly examined in the paper. A criminal offense and an infringement on the privacy of people and companies.

It should be mentioned that a number of research, reports, and surveys frequently cite facts and numbers that highlight the rising prevalence and rate of identity theft in the digital and electronic environment. While many of these studies will be mentioned throughout the current study, only a few of the most recent and convincing pieces of evidence that indicate this factor will be mentioned. This thesis will also reference numerous other general overviews and research of the effects of identity theft. The influence of identity theft on the developing ecommerce processes and markets is one locus that may be used as a baseline, so to speak, in the literature, despite the fact that there are numerous general studies covering a vast and diversified range of information in this sector. Due to consumer appeal and the growing significance of online commerce and shopping for all types and shades of entrepreneurship and business, current research on identity theft is concentrated in this field. As a result, this topic has received more attention from researchers than any other.

One should also be aware of the abundance of information from reputable and verified sources on the Internet when it comes to online shopping and ID theft. It is reasonable to assume that e-commerce professionals and internet pundits will be particularly interested in this topic. Online Privacy and Security: The Fear Factor (2006) from the well-known e-marketer Web site is one study that has to be addressed in this context. For experts in this field, this particular site also offers comprehensive and current statistics and viewpoints.

OFT launches fact-finding market study on online shopping, which is another helpful resource. The Office of Fair Trading has just released a new fact-finding study on internet purchasing, according to this story from the UK government website. (OFT starts an investigational market research on online purchasing) The website offers a lot of information on the influences on e-commerce and the effects of identity theft.

Reports from research firms like Gartner also turned out to be a trustworthy and significant addition to the study of this subject. By keeping track of the most recent information on identity theft news and statistics, other research firms like CyberSource also offer a crucial service. Weblogs are a very vital method of ingesting and compiling crucial information on this subject, and their significance cannot be understated. Weblogs would have been seen as a very dubious data source even a year ago. Weblogs have developed more recently, and many of the experts now use them as reliable sources of information. The Dent Weblogs, for instance, compile and cite reports and white papers from research firms like CyberSource. The Zante weblog, for instance, cites a report from CyberSource that states: "Statistics and data abound on the numerous security breaches and infringements, as well as many forms of online retail fraud. For instance, according to research firm Gartner, computer fraud grew 28% in the year that ended in May 2005.

A total of 73 million adults claim to have received a phishing email or a message that appeared to be one. A total of about $929 million was lost by over 2 million people. [5] Specialist Weblogs have thus developed into a useful method of keeping track of multiple sources, and as a result, they are a legitimate and significant component of the literature on this subject. It is important to keep in mind that only the most reputable and peer-reviewed blogs can be used for research and that in some circumstances, the veracity of data on blogs is still subject to question. The literature has a variety of topics that require further in-depth study, as was already noted earlier in this section. Pundits also point out that relatively little study has been done on the connection between consumer risk perceptions and privacy and security concerns. According to Miyazaki and Fernandez, this area of research has also disregarded how the perception of this link influences consumer behavior. [6] Indeed, a recent survey of Internet users was not quite decisive when it came to the effect of customer worries over privacy and security on online purchases. [7] Numerous studies also suggest that e-primary commerce's issue today is security, particularly as it relates to online purchases and strategies for protecting transaction privacy. There is a growing understanding that security concerns must be addressed in order to increase consumer confidence and lessen the impression of risk in online sales in order for ecommerce to realize its full potential. Additionally, it is seen to be crucial for the public to witness the efforts made by businesses in this area and for there to be less of an undercurrent of skepticism and mistrust about online transactions.

There is concern that if this goal is not met, media reports and other sources may heighten security concerns and discourage online shopping. According to Miyazaki and Krishnamurthy's study from 2002, "Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions," changes in online retailers' business practices that are thought to be customer-friendly will increase consumers' confidence and lower their perception of risk as they come into contact with them through more frequent Internet use. On the other hand, by highlighting the possible hazards associated with online buying, media coverage of these concerns and bad online experiences may lower consumer trust and discourage Internet users from making online purchases (Judge 1998). The subject of the expenses that identity thefts suffer is one area of the literature that is important in terms of the individual as well as industry and government. The report Tackling Phishing: Costs of Identity Theft to Financial Institutions provides insight into the repercussions. Despite the Never-Ending Battle, the Anti-Fraud Arsenal Keeps Increasing by Wetzel (2005). An excerpt from this study emphasizes how serious this problem is. This refers to the hidden costs associated with the decline in client confidence brought on by ID theft, in addition to the obvious costs to institutions like banks.

Phishing is reducing customers' faith in online contacts with their banks, according to a poll of 650 U.S. banking clients conducted in April 2004 by software provider Coyote. According to the survey, phishing made account holders less likely to use their bank's online services (65%) and respond to emails from their bank (75%), respectively. [8] Is eCommerce Boundary-Less? is a significant study that elaborates on the implications and effects of identity fraud. By Lim et al., "Effects of Individualism-Collectivism and Uncertainty Avoidance on Online Shopping" This article investigates the topic of consumers avoiding online shopping and trade because they fear identity theft. [9]

Mobile fraud, ID theft in mobile computing, and mobile phone fraud are other topics in the literature on ID theft that are expanding exponentially. This is a brand-new topic that will be covered in the chapters to follow. The recent expansion of the mobile sector and the corresponding growth of online commerce using mobile devices are significantly responsible for this field of study's growth. The expansion of this sector has created new potential for economic growth, but it has also opened up new paths and chances for identity theft.

This aspect of ID theft is the subject of an increasing number of credible research. For instance, the article Number Of Mobile Subscribers Worldwide To Rise To 3.96 Billion By 2011 explains the possible threat of security issues like identity theft in the expanding mobile business and provides some helpful background information. This is a particularly significant trend since it affects developing economies all across the world and is not only relevant to the United States. Growing Global Mobile Population expresses this plainly. "This trend does not simply affect Western nations or the United States. Even more subscriber bases and mobile ecommerce opportunities exist in China. According to In-Stat/MDR, revenues from Chinese handsets reached about $9 billion in 2003, and predictions indicate that they will reach $16 billion by 2008. (Growing Global Mobile Population) Windows Wi-Fi attack discovered by Espinar is a further investigation that is pertinent in this regard (2006) [10]

Literature on combating the problem of identity theft. The literature on preventative methods and techniques for ID theft is possibly one of the most important areas of research and one where there is a great amount of debate and discussion. It is also the most important area of research in terms of the aimsand objectives of the present study. There are numerous studies that have emerged in recent years whichfocus on solutions to the problem of identity theft. While there are a lot of ideas and suggestions, the majority of research identify identity theft as a persistent issue that uses the most recent technologies. Finding ways to counter this danger therefore necessitates understanding how the most recent technologies function as well as their flaws and potential exploits.

Tackling Phishing: The Problem and Complications of Addressing This Issue is a research that examines phishing practices, the issue, and the challenges of resolving this matter. The Fight Against Fraud Is A Never-Ending One By Rebecca Wetzel, "Arsenal Keeps Growing" ( 2005) In addition to providing a concise overview of the issue with ID fraud and phishing, this article also discusses possible solutions and activities that can be taken to lessen the threat. Other works that address the topic of privacy protections and preventive measures include What If the Virtual Walls Fall? by Klein et al. and Anticipating the Worst of Times by James Radford (2001). (2006) [11]

Consumer's Protection of Online Privacy and Identity by Milne et al. is a research that examines the numerous methods in which a person might defend themselves against invasion and identity theft (2004). This article is an excellent illustration of a study that explores the several alternatives available to computer users to safeguard themselves against identity theft. Additionally, there is a growing body of research that examines the initiatives taken by the government and governmental organizations to address the issue of ID theft. Of course, one must include the numerous analyses and critiques of FACTA, or The Fair and Accurate Credit Transactions Act of 2003, in this category of literature. This important Bill is one of the main attempts by government to develop a policy to counteract identity theft and fraud in the country.

There have been many reviews of this Act, both positive and negative, as can be expected in an internet world and economy that are continuously changing. In the portions of this thesis that follow, this topic will be covered in more detail. Identity Theft Legislation: The Fair and Accurate Credit Transactions Act of 2003 and the Road Not Taken, by Stefan Linnoff and Jeff Langenderfer (2004), is one study that has been found to be particularly helpful in providing an overview of this Bill's intentions as well as in discussing the various practical advantages and disadvantages of the Act. This article offers a thorough analysis of the 2003 Fair and Accurate Credit Transactions Act (FACTA). [12]

The role that larger organizations can play in the prevention of identity theft is a related topic that will also be of interest in this study. Numerous studies in this area advocate the idea that larger corporations and institutions, including banks, have a duty to the user to see to it that steps are taken to lessen fraud and identity theft. The Role of Organizations in Identity Theft Response by Lacey, D. and Ganesan, S. (2004) is a helpful research that covers a lot of the territory of this topic area. In a similar line, other studies claim that a synergistic and integrative approach and plan, which incorporates the full participation of all people affected by ID theft, is the only effective and feasible response to identity theft. This is a significant issue that will make up a large portion of the current study's attention.

Numerous journal papers and research have been published that discuss both the effects of ID theft and the preventative steps that can be implemented. They consist of the following: By David Breitkopf, Identity Theft Really Affects Your Lifestyle (2003) Identity Theft: Investigation and Preventative Tools from the 2006 National Community, and Identity Theft Survey Report, both produced by Sy novate (Aegis Group plc). [13]

Given the importance of the Internet in our daily lives and the fact that many of our common things can be connected to it, cybersecurity has grown to be a big worry in today's society. It can be accessed if it can be connected. Therefore, intrusion detection, which involves monitoring physical or cloud computer operations through analysis of system vulnerabilities and activity patterns, is the main concern for cybersecurity. Attacks could take the form of data manipulation, malicious IPs, or distributed denial of service, for example, with consequences include information loss, business losses, and physical harm. You may think of the internet of things as a brand-new concept that unites both the current internet and tangible objects.

For instance, when we talk about "smart houses," we're talking about home automation, manufacturing systems, or the industrial process, and health, or hospital automation. [9] In this way, the internet of things significantly enhances the numerous gadgets and connected equipment in our life, such as smart grids and electric vehicles for transportation. Therefore, despite offering a wealth of benefits, internet technology also offers a significant risk. As a result, applications for internet of things include a wide variety of artifacts, including smart grids, massive smart factories, and smart households. In each instance, the corresponding devices are enhanced by wireless sensor network interfaces, which are a crucial internet of things technology for the vast array of IoT systems. Examples include “smart grid”, “Internet of Things”, “manufacturing systems”, “smart cities”, and “cloud computing in transport and smart homes”.[14]

On the one hand, in the case of smart homes, it is advised to keep the software up to date from reputable suppliers and cloud providers while protecting sensors' identities from being recognized through wireless communication environment networks. The internet of things, on the other hand, provides a variety of services in smart cities, where many people will likely move. These services include smart parking, environmental, waste, water, and traffic management, as well as monitoring energy consumption. These operations span the internet of things spectrum, its energy and architecture efficiency, and mitigating its environmental effects while keeping in mind its context interplay. [15]

The internet of things offers a variety of subtle differences from the conventional internet of things. The Internet functions in an industrial environment, whereas the internet of things operates in a household setting. In this approach, it includes things like supply chain optimization. The term "Industry 4.0," which refers to technology and value chain organization ideas, is synonymous with the internet. The modular structure of Industry 4.0 allows computers to monitor and control smart factories and the physical processes that flow from them, generating a digital replica of those operations while making decentralized decisions. Along the route, interactions between computers and people happen. Concerns about IoT in general and cybersecurity are both included in the internet of things. It emphasizes data integrity, which prevents unauthorized parties from altering it, authentication, which ensures that the data source is the claimed identity, privacy, which prevents unauthorized parties from tracing users' identities through their actions, confidentiality, which renders information incomprehensible to them, and availability, which limits access to system services to authorized users. IOT thus confronts significant difficulties, particularly when operating in decentralized environments like Blockchain systems and the variety of smart artifacts. Also worth emphasizing are the diverse sensors' limited processing capabilities and power, which make conventional security measures ineffective. The aforementioned problems increase the likelihood of cyberattacks on IoT systems, such as transportation, home appliances, and manufacturing plants. As a result, there is a significant need for improvement in remote system authentication, new sensor encryption, and intrusion detection web interface and software. Additionally, as IoT innovation grows, wireless technologies become more advanced and open up a wide range of opportunities, such as 5G, which is designed for much more than just speech and data. [16]

In relation to the internet of things, the literature study that is presented here offers a number of security recommendations for cordless sensor networks. In particular, decentralized architectures composed of numerous objects, like Blockchain and cloud computing systems, make it easier to manage and configure networks. They also improve IoT security by utilizing sensors that improve data transmission and by preventing wireless channel redundancy through the use of big data systems. A preliminary Scopus search using the terms "Internet of Things" and "Cyber Security" produced the design of the conceptual and technological framework for this paper, which is displayed and explored in the following parts. [17]

Cybersecurity is concerned with the methods by which systems are accessed as well as the protection of hardware, software, and data. Security goals typically include privacy, which refers to preventing unauthorized devices or people from accessing, altering, or destroying information [18]. As a result of the vast number of IoT-based linked devices now in existence, society is also growing more open to cyberattacks, such as denial-of-service attacks by insiders and hackers that prevent direct access to devices, etc. As technology becomes more prevalent in our daily lives, cybercrime and cybersecurity tools also advance at the same time, requiring investments in cybersecurity defenses from the entire manufacturing sector as well as new IoT cybersecurity management solutions. [19] Additionally, because major infrastructure components are so sensitive and expensive to hack, cyberattacks on smart grids have a significant negative impact on public safety. The absence of efficient defenses, such as cybersecurity professionals, is causing increased anxiety about cybersecurity. For instance, China is developing new cybersecurity legislation and policies. Healthcare is a hot topic right now since there is a ton of vital data, but hospitals typically have insufficient cyber security, putting patients' lives and trust in danger. There is a knowledge gap about frameworks to address the complex cybersecurity issues in the internet of things because prior literature has concentrated on the technical aspects of cybersecurity. A survey of the literature on IoT security technology and cyber risk management in industry is provided by this study. [20]

These days, this type of technology is used in a wide range of industries, including the health, energy, and transportation sectors [21]. By 2020, more than 28 billion IoT devices will be able to connect to the Internet, predicts Gartner. By 2020, it is predicted that there will be 7.8 billion people on the planet. As a result, each person will have an average of three devices that can connect to the Internet. The word "IoT" has been defined by numerous standards bodies from both academic and business. We offer a definition of the International Telecommunication Union in this essay. A global information society infrastructure that "enables sophisticated services by connecting (physical and virtual) things based on existing and developing, interoperable information and communication technologies." [22] The IoT is nevertheless susceptible to a variety of security risks and vulnerabilities, just like any other communication network. The development of the Internet of Things faces significant security challenges in particular because it combines several technologies, including wireless sensor networks, optical networks, mobile broadband, and 2G and 3G communication networks, and represents an extension of the traditional unsecured Internet model. The aforementioned technologies are all subject to different security vulnerabilities. Additionally, the IoT gadgets can interact with their surroundings automatically and autonomously without any outside influence, which has led to a variety of security concerns.

Last but not least, the numerous connections between users and objects or between objects produce enormous amounts of data that are challenging to handle. When the affected user has not revealed the cause of their own victimization, problems can arise. The real story behind the compromised user is that they considered their own investments for the argument that those who are unidentified and insecure are stacked on the same life cycle.

Numerous research have looked at the security vulnerabilities in the IoT for the aforementioned reasons. Some of them decide what security needs and difficulties the Internet of Things brings about. Other research identifies potential dangers, weaknesses, and defenses. Additionally, a lot of articles look at IoT protocol security challenges, while others concentrate on certain security processes and mechanisms that can reduce the risk of intrusions. The next section includes a brief description of a few of these cases. Even if these works provide substantial and essential contributions, the continual evolution of cyberattacks necessitates the concurrent investigation of adequate responses, making thorough survey articles necessary and helpful.

## 3. Methodology

The research goal refers to the overarching objective that has to be accomplished by carrying out the research. It could be to contribute to the existing body of knowledge in the field, to close a knowledge gap, to create and test a solution to a problem, or for any number of other reasons. In this chapter, we discussed the strategies that we put into practice in order to accumulate and broaden our knowledge. The overall appearance and feel of the thesis work. This chapter discusses the methodology of the research as well as a general overview of the relevant theory. Among the steps of this study present situation of cyber security issue in all over the world. This study is part of a larger research project. A review of thefindings of prior research, the creation of a questionnaire for a survey, qualitative and quantitative analysis based on the survey review, survey results,

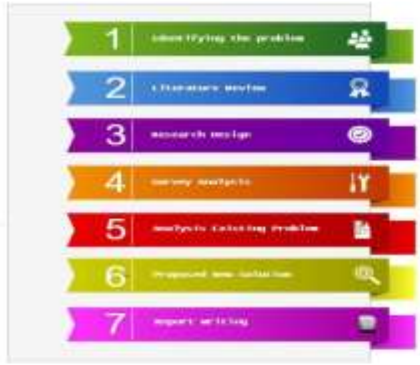

Figure3. 1: Procedure of the Research

### 3.1 Research Analysis

ID theft has increased dramatically with the development of the Internet and e-commerce. Thieves deceive unwary computer users into submitting personal information using readily available Internet tools, which they subsequently utilize for illegal activities. The possibility of fraud is a significant barrier to the development and expansion of internet commerce. Public suspicion of e-payment and e-banking services, the book's main subject, is severe. Numerous OECD members have taken action to make sure that customers and Internet users are sufficiently safeguarded in light of the rise in online identity theft. These steps include a variety of actions, including campaigns to raise consumer and user awareness, new legal frameworks, public-private collaborations, and industry-led technical response projects.

### 3.2 Interpret and Research Proposal

Due to numerous public occurrences in the United States, the objective of raising awareness of identity theft is at an all-time high. The consequences for the particular victims of identity theft are, at best, time-consuming and frustrating, and, worst of all, they may harm their financial histories. Another group of victims, including merchants and financial institutions, have also had to bear the financial burden of millions of dollars as a result of identity theft fraud. Because businesses entrusted with people's personally identifying information (PII) did not sufficiently protect that information, several of the recent newsworthy identity theft incidents happened. A business's misuse of PII data may result in major financial losses, a decline in customer, partner, employee, and shareholder trust, significant quantities of negative news, and even criminal charges, according to recent legislation requiring public notification of such instances.

## 4. Analysis and Proposed Model

In this chapter thesis describe it self about the domain of identity theft on internet its existing analysis and its solution end of the section it is proposed new model. New model will be described new innovativesolution to find the theft on internet. From the literature review this thesis find the exiting solution of domain. Most recently internet has been recorded that the internet fraud and cyber-attack on banking systems. The culprits are hide themselves using internet and do their illegal activity to make system vulnerable and massacre. This thesis also looking for a existing solution of exiting problem and apart from it thesis will discover new model of solution.

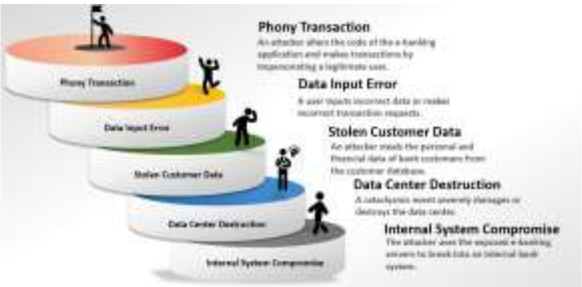
Phony Transaction
An attacker alters the code of the e-banking application and makes transactions by impersonating a legitimate user.
Data Input Error
A user inputs incorrect data or makes incorrect transaction requests.
Stolen Customer Data
An attacker steals the personal and financial data of bank customers from the customer database.
Data Center Destruction
A cataclysmic event severely damages or destroys the data center.
Internal System Compromise
The attacker uses the exposed e-banking servers to break into an internal bank system.
Phony Transaction
Data Input Error
Stolen Customer Data
Data Center Destruction
Internal System Compromise

Figure 4. 1:Basic Process of Identity or Data Lose.

### 4.1 Identity Theft Existing Analysis:

In this section thesis define itself is the existing problem on identity theft on internet. In this wide worldno one can imagine in their seconds of life without internet. People are trying to make their lives advanceand easier that’s why every work has done over using the internet. But Some of people are using this in wrong way. This makes life and worse in general people. Information compromise and accounts corruptby third party is most dangerous cyber-attack in current situation. In recent years a massive attack took place in an organization of a country which direct involved in the country reserve. The process was followed by the hackers are very in simply way, just followed some steps they compromise the whole security system of an organization. The steps were,

Social Engineering , Network Monitoring , Malware Attack

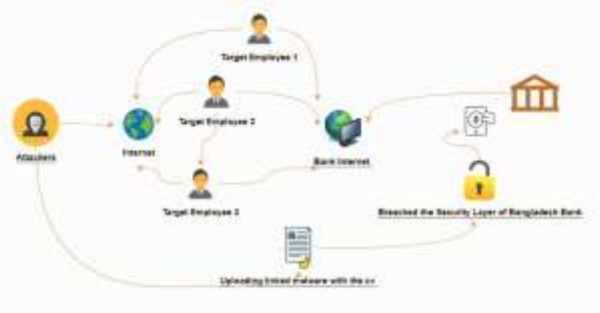
Target Employee 1
Target Employee 2
Attackers
Internet
Bank Internet
Target Employee 3
Breached the Security Layer of Bangladesh Bank
Uploading linked malware with the cv

Figure 4. 2:Model view of the Organization Attack Process

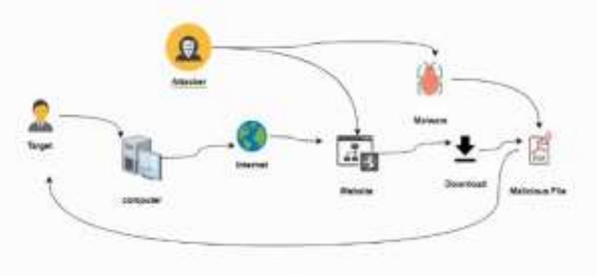

Figure 4. 3:Model View of Individual attack

### 4.2 Identity Theft Existing Solution:

In this chapter this paper describes the steps of taken by the authority of the target after the incidenthappened in 2016 cyber-attack on them which is already explained in details at previous chapter. Afterthe massive cyber-attack at the target. The target is connected to the countries reserve so that thegovernment setup multiple enquire committee. The main motive to create this committee is to find thereasons to this attack, find the attackers and proposed the strategies to prevent this type of attack in future.After the incident of the cyber-attack the governor of the country had resigned from his post. Thegovernor and the higher authority did not inform any one of the ministries of finance and also to prime minister or president. When the incident came out into the public, crime investigation department (CID)investigate the whole incident the governor and the authority were silent during the investigation. Thefinal report from the investigation team said that the former governor and senior officials were equallyresponsible for removing theft data. They hired a private IT firm to erase all the traces of the massive theft.

From this the authority still not disclose any information about the recovery system and setup any new parameter inside their vulnerable system in public, print media or any investigation panel.

### 4.3 Identity Theft New Proposed Model

Figure 4.4 :Model view of an organization can prevent the attack

From the figure 4.4 describe itself that the steps can be followed by and organization to prevent the attacks. The steps are not proper final solution of being attacked but also can help to awake and being alert of attack. Day by day the security vulnerabilities are coming out and attacking approaches are newlyintroduced but the below steps can save to lose your identity and primary attacked.

- Close coordinate with cyber threat intelligence team
- Before open/download any file from internet should check malware detect scanning.
- Multifactor authentication has been enabled for system whose are direct connected to all the important areas (e.g.: transaction, printing, user credentials).
- Setup specific network for specific user and work
- Segment networks and isolated remote access

The large number of cyber-attacks conduct in large organization. Vulnerability of any system can cost huge lose for any induvial or organization. For that security measurement and upgrading itself much needed. This thesis encouraged people of induvial and organization to up to date with technology and secure themselves from internet thieves to prevent their loosing data. In the time this paper introduced the process of being secure and way to using secure internet.

## 5. Conclusion

Identity theft is, in summary, unlawful, unethical, and extremely hazardous to the victim. This is due to the fact that identity theft can seriously harm the victim's family's finances and reputation. That there are so many instances of this crime in the world today is unfortunate. After considering everything, it is critical to take precautions to avoid identity theft. However, it is getting tougher and harder to do so as technology develops. It is crucial that everyone understands what identity theft is and what they can do to stop it because of this. Identity theft will decrease after this is done, and the world will be a better and safe place. The aforementioned study's components as well as the diverse viewpoints that were discovered during the inquiry can be summed up as follows. Business, consumers, organizations, and the government must all work together to combat the threat of identity theft in order to find a holistic solution to the growing challenges of identity theft.

This report summarized the most recent, cutting-edge research on computer crime (also known as cyber crime) and identified knowledge gaps. The main outcomes of this thorough research are to provide a complete overview of the toolkits used for each investigation into a cybercrime domain. We provided a thorough comparison of the various cybercrime domains and developed a grading methodology based on several aspects for both commercial and free toolkits to assist investigators in selecting the best toolkit for a given circumstance. We compiled the 35 responses from respondents and displayed a summary in graphs and charts. Those results of our survey.

The literature review in this study and other sources have also stated that there is currently no integrated document to plan in place that defines such a comprehensive and integrated picture of the situation. The purpose of this essay was to urge a redefining of identity theft from an aggravating situation, a tool for other crimes, and an autonomous concept that should take into account the user's virtual identity. However, if we acknowledge that the IP address is a component of this identification, the troubling issue of IP theft pertains more to the traditional method than the modern one. This means that the new strategy must be viewed as a second layer of user protection that complements rather than replaces the traditional strategy. It's crucial to keep in mind that the preservation of one's identity is the basis of every civilized society at this time when many are concerned about the possibility of the internet turning into a war zone. Therefore, the research generally tends to imply that focused efforts should be undertaken to gain a deeper grasp of the context and its scope.

## Bibliography

[1] $2.8 bln in e-commerce revenues lost to fraud in 2005; available from http://blogs.zdnet.com/ITFacts/index.php?cat=33&paged=2; Internet; accessed17 November 2006.

[2] 2 billion mobile subscribers by end of 05; available fromhttp://www.smartmobs.com/archive/2005/08/25/2_billion_mobil.html; Internet; accessed17 November 2006.

[3] 74% IT managers receive phishing attacks; available from http://www.financialexpress.com/fe_full_story.php?content_id=98848 ;Internet; accessed 17 November 2006

[4] 207K complaints on cyberfraud logged in 2004; available from http://blogs.zdnet.com/ITFacts/?p=9372; Internet; accessed17 November 2006

Adkins S. 2005. Internet Security Threats Will Affect U.S. Consumers' Holiday Shopping Online; available from http://www.bbb.org/Alerts/article.asp?ID=637; Internet; accessed 17 November 2006

[5] Anonymizer Now Protects Against Pharming Attacks; available from http://www.marketwire.com/mw/release_html_b1?release_id=85321; Internet; accessed13 November2006

[6] Bielski, L. 2005. Security Breaches Hitting Home: Phishing, Information Leaks Keep Security Concerns at Red Alert. ABA Banking Journal, 97(6), 7.

[7] Bielski, Lauren. 2006."Debit's Growing Popularity." ABA Banking Journal 98.1: 37.

[8] Blair, Kevin. 2001."Moving Fast: Competition Heats Up on Credit Card Security." ABA Banking Journal 93.4 (2001): 63.

[9] Britons 'dependent on mobile use'; available fromhttp://news.bbc.co.uk/2/hi/ business/5204454.stm;

Internet; accessed 17 November 2006

[10] Cookies; available from http://www.webopedia.com/TERM/c/cookie.html; Internet; accessed 13November 2006.

[11] Cox. J. 2006. Mobile users face knotty security issues; available from http://www.networkworld.com/news/2006/071706-mobile-users-security.html?fsrc=rsssecurity; Internet; accessed13 November 2006.

[12] Baird, & Mayer, D. (2021). On integrative social contracts theory and corporate decision-making in a polarized political economy. Business and Society Review (1974), 126(1), 3–23. https://doi.org/10.1111/basr.12223

[13] Espiner T. Windows Wi-Fi attack discovered 2006; available from http://news.zdnet.co.uk/0,39020330,39247302,00.htm; Internet; accessed18 November 2006

[14] Internet Commerce Grows 88 Percent by Dollar Volume and 39 Percent by Transaction Volume: Fraud Remains a Concern; available from http://www.verisign.com/verisign-inc/news-and-events/news- archive/us-news-2005/page _028572.html; Internet; accessed 17 November 2006

[15] Gips, Michael A. "Security Management Online." Security Management Dec. 2000: 16.

[16] Han J. One in Four Computer Users Hit by Phishing Attempts

[17] Each Month, According to Major In-Home Computer Safety Study; available from http://www.staysafeonline.info/news/press_dec07_2005.html; Internet; accessed15 November 2006.

[18] Identity Theft Survey Report. Prepared by Synovate (Aegis Group plc) ; available from http://www.ftc.gov/os/2003/09/synovatereport.pdf; Internet; accessed15 November 2006

[19] Lacey, D., & Cuganesan, S. 2004. The Role of Organizations in Identity Theft Response: The Organization-Individual Victim Dynamic. Journal of Consumer Affairs, 38(2), 244+.

[20] Lim, Kai H., Kwok Leung, Choon Ling Sia, and Matthew K.O. Lee. 2004. "Is eCommerce Boundary-Less? Effects of Individualism-Collectivism and Uncertainty Avoidance on Internet Shopping." Journal of International Business Studies 35.6 (2004): 545+

[21] Malicious Software Expected to Increase; available from http://www.wirelessweek.com/article/CA6299498.html?spacedesc=Departments: Internet; accessed15November 2006.